УДК 519.72

О СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПРОБЛЕМЫ РЮКЗАКА

В.О. Осипян

Кубанский госуниверситет, г. Краснодар
E-mail: rrwo@mail.ru

Показана возможность обобщения базовых рюкзачных систем защиты информации. Приводится алгоритм построения инъективного нестандартного рюкзака размерности n+1 с заданными каскадными значениями, исходя из аналогичного рюкзака размерности n. В работе рассмотрена лёгкая задача укладки нестандартного рюкзака.

Как известно [1–3], криптостойкость рюкзачных систем защиты информации (РСЗИ) на основе заданного рюкзака зависит от первоначального способа кодирования элементарных сообщений и процедуры последующего шифрования открытого текста.

Рассмотрим класс систем защиты информации с открытым ключом и с рюкзаком, обладающим заранее заданными свойствами. Рюкзачный вектор $\boldsymbol{A}$ назовём с повторениями или без повторений, если его элементы повторяются или нет – соответственно. Для простоты изложения будем считать, что значения компонент рюкзачного вектора расположены в неубывающем порядке своих значений. При этом коэффициенты повторов для компонент рюкзака и входа $(\boldsymbol{A}, v)$ можно взять совершенно различными между собой способами из заданных двух целочисленных положительных массивов.

Пусть $\boldsymbol{A}=(a_1,a_2,...,a_n)$ – рюкзачный вектор размерности n, $n\geq3$ из n натуральных компонентов a_i, $i=1...n$ и $(\boldsymbol{A}, v)$ – вход задачи о рюкзаке, где v – также некоторое натуральное число или нуль. Пусть далее, $ZK_t=\{k_1,k_2,...,k_t\}$, $k_1+k_2+...+k_t=n$, $t\leq n$, $ZC_p=\{m_1,m_2,...,m_n\}$ – множества коэффициентов повторений компонентов рюкзачного вектора $\boldsymbol{A}$ и входа $(\boldsymbol{A}, v)$ соответственно. Здесь элемент k_i, $k_i\geq1$, $i=1...t$ – количество повторений компонентов ранга натурального числа a_i в рюкзаке $\boldsymbol{A}$ (t – количество его различных компонентов), а элемент m_i, $0\leq m_i\leq p-1$, $i=1...n$, $p\geq2$, $p\in N$ из множества ZC_p указывает максимальное значение коэффициента повтора при a_i, $i=1...n$ для определения входа $(\boldsymbol{A}, v)$. Множества ZK_t и ZC_p назовём спектрами коэффициентов рюкзака $\boldsymbol{A}$ и его входа $(\boldsymbol{A}, v)$ соответственно. Значения множества ZC_p иначе назовём каскадными значениями.

Так, например, если t=4, p=3 и

$$A=(1, 2, 5, 5, 13, 13, 13),\ ZC_3=\{1, 1, 1, 2, 2, 2, 1\},$$

то спектр коэффициентов рюкзака имеет вид

$$ZK_4=\{1, 1, 2, 3\},\ k_1=1,\ k_2=1,\ k_5=2,\ k_{13}=3,$$

а спектр входа задан как ZC_3, для которого каскадные значения заданы как:

$$m_1\le1,\ m_2\le1,\ m_3\le1,\ m_4\le2,\ m_5\le2,\ m_6\le2,\ m_7\le1.$$

Аналогично определим: решением без повторений компонент для входа ($\boldsymbol{A}$, v) назовем подмножество элементов $\boldsymbol{A}$, сумма которых равна v, т.е.

$$\sum_{i=1}^{n}\alpha_i a_i = v,$$

при условии, что $\alpha_1\in\{0,1\}$ – как принято считать для стандартных рюкзачных систем. Если же α_i-$\in ZC_p=\{m_1,m_2,...,m_n\}$ и хотя бы один из коэффициентов $\alpha_1\ge2$, то решением – соответственно с коэффициентами повторений компонент из ZC_p.

Все рассматриваемые в данной работе рюкзаки вовсе не обязаны обладать свойствами, присущими стандартным рюкзакам. Наоборот, здесь a_i, $a_i\in ZK_t$ может повторяться и входить в сумму для определения входа ($\boldsymbol{A}$, v) с коэффициентом $\alpha_i\le m_i$, i=1...n, где $m_i\in ZC_p$. Такие нестандартные рюкзаки обозначим через $\tilde{A}$, а входы – соответственно ($\tilde{A}$, v).

Очевидно, в частности, если для нестандартного рюкзачного вектора $\tilde{A}$

$$k_1=k_2=...=k_n=1,$$
$$m_1=m_2=\ ...=m_n=1,$$

то мы имеем стандартный рюкзак без повторений [1]. Если же при $k_1=k_2=...=k_n=1$, соответствующие им коэффициенты входа $m_1=m_2=\ ...=m_n=1$, то мы имеем обобщённый рюкзак [4] с заданным максимальным числом $p-1$ повторений всех его компонентов.

Множество значений v_i, для которых входы ($\tilde{A}$, v_i) со спектром ZC_p имеют решения, назовем допустимыми значениями и обозначим через $V_{\tilde{A}}=\{v_0,v_1,...,v_t\}$. Количество всех допустимых числовых значений v_i для нестандартного рюкзачного вектора $\tilde{A}$ обозначим через $\mu(V_{\tilde{A}})$ и назовём мощностью входа. Так как для одного и того же v_i могут быть разные решения, то обозначим через $\mu(\tilde{A})$ мощность различных между собой решений и назовём его мощностью нестандартного рюкзака $\tilde{A}$. Вектор $\tilde{A}$ назовём инъективным, если каждый его вход обладает не более чем одним решением – с повторениями или без него. Очевидно, для инъективного вектора $\tilde{A}$ имеет место равенство:

$$\mu(V_{\tilde{A}})=\mu(\tilde{A})=(m_1+1)(m_2+1)...(m_n+1).$$

Более того, имеет место также соотношение:

$$m_1a_1+m_2a_2+...+m_na_n=\frac{2}{\mu(\tilde{A})}\sum_{i=0}^{\mu(\tilde{A})-1}v_i,$$

откуда в частности следует, если:

1. $\tilde{A}$ – стандартный рюкзак, то $m_1=m_2=...=m_n=1$, $\mu(\tilde{A})=2n$, следовательно, $a_1+a_2+...+a_n=\frac{1}{2^{n-1}}\sum_{i=0}^{2^n-1}v_i$;
2. $\tilde{A}$ – обобщенный рюкзак, то $m_1=m_2=...=m_n=p-1$, $\mu(\tilde{A})=p^n$ и

$$a_1+a_2+...+a_n=\frac{2}{p^n(p-1)}\sum_{i=0}^{p^n-1}v_i.$$

Последние соотношения можно применить для установления инъективности нестандартного вектора $\tilde{A}$, а с помощью следующего рекуррентного алгоритма легко найти множество всех допустимых значений v_i со спектром входа ZC_p и определить a_{n+1}, если известны $a_1,a_2,...,a_n$. Для удобства приведём схему построения такого алгоритма, представленной в виде таблицы (см. табл) значений для коэффициентов компонентов нестандартного рюкзака. Из таблицы видно как найти всевозможные наборы длины n+1 и соответствующие им значения v_i, если известны наборы длины n.

Таблица. *Схема построения алгоритма*

a_{n+1}	a_n	a_{n-1}	...	a_0	a_1	v_i
0	0	0	...	0	0	0
0	0	0	...	0	1	a_1
0	0	0	...	0	2	$2a_1$
			. . .			
0	0	0	. . .	0	m_1	m_1a_1
0	0	0	. . .	1	0	a_2
0	0	0	. . .	m_2	m_1	$m_1a_1+m_2a_2$
			. . .			
0	m_n	m_{n-1}	. . .	m_2	m_1	$m_1a_1+...+m_na_n$
1	0	0	. . .	0	0	a_n+1
1	0	0	. . .	0	1	a_n+1+a_1
1	0	0	. . .	0	2	a_n+1+2a_1
			. . .			
1	0	0	. . .	0	m_1	$a_n+1+m_1a_1$
1	0	0	. . .	1	0	a_n+1+a_2
			. . .			
1	0	0	. . .	m_2	m_1	$a_n+1+...+\ m_2a_2+\ +m_1a_1$
			. . .			
m_{n+1}	m_n	m_{n-1}	. . .	m_2	m_1	$m_1a_1+...+m_n+1a_n+1$

Итак, пусть

$$\tilde{A}=(a_1,a_2,...,a_n)$$

– нестандартный рюкзачный вектор размерности n, $n\ge3$ из n произвольных натуральных компонентов a_i, i=1...n, ($\tilde{A}$, v) – его вход со спектром входа ZC_p и

$$v=\sum_{I=1}^{n}\alpha_I a_I=\tilde{A}\cdot w_v^T$$

– произвольное допустимое значение для входа ($\tilde{A}$, v). Здесь и ниже будем считать, что k_i=1, i=1...n, т.е. заданный нестандартный рюкзак $\tilde{A}$ без повторений.

Пусть, далее, $V_{\tilde{A}}$ – множество всех допустимых значений v_i инъективного рюкзачного вектора $\tilde{A}$ размерности n, со спектром входа ZC_p, т.е.

$$V_{\tilde{A}}=\{v_0,\ v_1,\ ...\ ,v_{\mu(V_{\tilde{A}})-1}\},$$

а $\quad V_{\tilde{A}}+a=\{v_0+a, v_1+a,...,v_{m(V_{\tilde{A}})\text{-}1}+a\}$

– множество всех значений v_i со сдвигом на натуральное число a. Тогда

$$V_{\tilde{A}+1} = \bigcup_{u=0}^{m_{n+1}} (V_{\tilde{A}} + u\, a_{n+1})$$

– представляет собой множество всех допустимых значений для рюкзачного вектора $\tilde{A}+1$ размерности $n+1$ со спектром входа

$$ZC_p=\{m_1,m_2,...,m_n,m_{n+1}\}.$$

Поэтому для определения компонента a_{n+1} инъективного рюкзачного вектора $\tilde{A}+1$ размерности $n+1$ с каскадным значением m_{n+1}, необходимо и достаточно выполнение следующих двух условий:

1. $a_n < a_{n+1} < \sum_{u=1}^{n} a_u$;

2. $V_{\tilde{A}} \bigcap \bigcup_{u=1}^{m_{n+1}} (V_{\tilde{A}} + u\, a_{n+1}) = \varnothing.$

Таким образом, на основе указанного рекуррентного алгоритма можно найти все инъективные вектора размерности $n+1$, исходя из аналогичных векторов размерности n.

Рюкзачный вектор

$$\tilde{A}=(a_1,a_2,...,a_n)$$

назовём сверхрастущим, если для любого $j=2...n$ имеет место неравенство

$$a_j > \sum_{k=1}^{J-1} m_k a_k. \qquad (1)$$

Очевидно, если рюкзачный вектор $\tilde{A}$ сверхрастущий, то он инъективный и одновременно возрастающий.

В самом деле, так как мы имеем следующий диапазон значений для v:

$$0 \le v \le m_1a_1+m_2a_2+...+m_na_n,$$

то очевидно, если v не принадлежит указанному диапазону, то вход ($\tilde{A}$, v) не имеет решений. Не имеют решений и те входы ($\tilde{A}$, v), для которых v не представляется в виде линейной комбинации:

$$v=\alpha_1a_1+\alpha_2a_2+...+\alpha_na_n, \alpha_i \in ZC_p. \qquad (2)$$

Если же v имеет вид (2), и компоненты рюкзака $\tilde{A}$ удовлетворяют (1), то каждый из $\mu(V_{\tilde{A}})$ различных входа ($\tilde{A}_P$, v) имеет одно единственное решение в силу того, что заданный рюкзачный вектор сверхрастущий. Далее, будем говорить, что компонент a_i, $i=1...n$ входит в сумму v с кратностью $\alpha_i \in \{m_1,m_2,...,m_n\}$, если a_i имеет α_i вхождений в v. Аналогично можно ввести другие известные определения и обозначения для рассматриваемого вектора так, как, например, в работе [4].

В частности, аналогично можно доказать следующие теоремы относительно нестандартного рюкзака $\tilde{A}$ без повторений.

Теорема 1. Рюкзачный вектор без повторений $\tilde{A}=(a_1,a_2,...,a_n)$ размерности n, $n \ge 3$ с каскадными значениями $ZC_p=\{m_1,m_2,...,m_n\}$ для входа ($\tilde{A}$, v) является плотным и инъективным, если

$a_1=c$, $a_j=m^{j-2}((m-1)c+1)$, $j=2...n$, $m=\max\{m_1,m_2,...,m_n\}$, $m \in 1$, где c – некоторая целая положительная константа.

Доказательство. Так как из указанного рекуррентного соотношения при $n \ge 3$ непосредственно следует, что

$$a_j=ma_{j-1}=(m-1)a_{j-1}+a_{j-1},$$

то имеем:

$$a_j=m^{j-2}((m-1)c+1)=(m-1)a_{j-1}+a_{j-1}=$$
$$=(m-1)a_{j-1}+((m-1)a_{j-2}+a_{j-2}=$$
$$...$$
$$=(m-1)a_{j-1}+(m-1)a_{j-2}+ ... +(m-1)a_2+(m-1)a_1+1.$$

Или

$$a_j = (m-1)\sum_{k=1}^{J-1} a_k + 1.$$

Таким образом, рюкзачный вектор $\tilde{A}$ – сверхрастущий, следовательно, и инъективен, причём разность между левой и правой частями полученного равенства, как видно, минимальна и равна единице.

Следствие. В частности, при $c=1$ из теоремы следует, что инъективный рюкзачный вектор

$$\tilde{A}=(1,m,m^2,...,m^{n-1})$$

является одновременно и плотным.

Заметим, что доказанная теорема справедлива также для более сильного условия, когда вместо m выступают соответствующие значения m_i, $i=1...n$, а на практике можно предложить следующий рекуррентный алгоритм построения инъективного (плотного) вектора $\tilde{A}+1$ размерности $n+1$ со спектром $ZC_p=\{m_1,m_2,...,m_n,m_{n+1}\}$, если известен аналогичный вектор $\tilde{A}=(a_1,a_2,...,a_n)$ размерности n ($n \ge 2$). Для этого необходимо определить очередной компонент а $n+1$ в виде:

$$a_{n+1}=m_1a_1+m_2a_2+...+m\text{n}a_n+a$$

так, чтобы выполнялось следующее очевидное равенство относительно мощностей:

$$\mu(V_{\tilde{A}+1}) = m_{n+1}\mu(V_{\tilde{A}}),$$

где

$$V_{\tilde{A}+1} = \bigcup_{k=0}^{m_{n+1}} (V_{\tilde{A}} + k\, a_{n+1}), V_{\tilde{A}} + a = \{v_0+a, v_1+a, ... ,v_t + a\},$$

$$a \in Z, \quad m_i \in ZC_p, \quad i = 1...n, \quad a_2 > a_1.$$

Теорема 2. Пусть

$$\tilde{A}=(a_1,a_2,...,a_n)$$

– инъективный рюкзачный вектор размерности n, $n \ge 3$, а вектор

$$\tilde{\mathbf{B}}=(b_1,b_2,...,b_n),\ b_i=e \cdot a_i(\text{mod}m),(m,e)=1$$

получен из $n \ge 3$ сильным модульным умножением относительно m и e. Тогда решение задачи о рюкзаке для входа ($\tilde{\mathbf{B}}$, $v \cdot e$) совпадает с единственным решением для входа ($\tilde{A}$, v).

Доказательство. Схема доказательства данной теоремы полностью совпадает со схемой построения алгоритма для стандартной рюкзачной системы. Разница лишь в том, что в качестве функции шифрования применяется функция

$$F(x) = \tilde{\mathbf{B}} W_X^T,$$

где WX – шифр сообщения X. Более того, алгоритм построения системы защиты информации с открытым ключом на основе рюкзака $\widetilde{A}$ полностью совпадает с алгоритмом построения систем защиты информации с обобщённым рюкзаком $\widetilde{A}_P$ [4].

Отметим, что данная теорема допускает все параметры обобщённой рюкзачной системы защиты информации с открытым ключом. При этом необходимо сделать ещё следующее замечание: процедура восстановления открытого текста, в целом, не зависит от самих компонент рюкзачного вектора $\widetilde{A}$, она зависит только от размера самого рюкзака и способа первоначального кодирования элементарных сообщений открытого текста. Данное замечание относится ко всем существующим открытым рюкзачным системам.

Совершенно ясно, если для нестандартного рюкзака $\widetilde{A}$ полагать что $m_1=m_2=...=m_n=p-1$, то все рассмотренные выше рассуждения относительно РСЗИ останутся в силе, что, в свою очередь, означает: их можно перенести на случай обобщённых рюкзаков $\widetilde{A}_P$ с заданным максимальным числом $p-1$ повторений всех его компонентов. Если же полагать $m_1=m_2=...=m_n=1$, то мы соответственно получим РСЗИ со стандартным рюкзаком.

В обоих случаях рюкзаки без повторений, т.е. $k_1=k_2=...=k_n=1$. Очевидно, когда компоненты рюкзачного вектор $\widetilde{A}$ с повторениями [5], т.е. хотя бы один элемент из множества $ZK_t=\{k_1,k_2,...,k_t\}$ больше единицы или то же самое, что $t<n$, то $\widetilde{A}$ в данном случае сверхрастущим быть не может, и потому невозможно рассмотреть лёгкую задачу укладки рюкзака и, тем более, задачу построения СЗИ, использующей такой рюкзак.

В заключение подчеркнём, что для больших значений параметров нестандартных рюкзачных векторов, криптостойкость соответствующих систем защиты информации сравнительно выше, чем криптостойкость аналогичных стандартных СЗИ. В самом деле, если обозначить через $N(K)$ – количество всех вариантов выбора ключей, то для стандартного рюкзака оно равно $N(K)=2^n$, для обобщённого рюкзака – $N(K)=P^n$, а для нестандартного рюкзака $\widetilde{A}$ – $N(K)=(m_1+1)(m_2+1)\ ...\ (m_n+1)$, где n – длина рюкзака.

СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 320 с.
2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
3. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001. – 260 с.
4. Осипян В.О. Об одном обобщении рюкзачных криптосистем // Известия вузов. Сев.-Кавк. регион. Техн. науки. – 2003. – Прилож. № 5. – С. 18–25.
5. Осипян В.О. О криптосистемах с заданным рюкзаком // Информационное противодействие угрозам терроризма. – 2004. – № 3. – С. 53–56.

УДК 681.326